UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/646,976	08/22/2003	Martin Lund	14218US02	1056

23446 7590 03/16/2011
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER
PAN, JOSEPH T

ART UNIT	PAPER NUMBER
2492	

MAIL DATE	DELIVERY MODE
03/16/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/646,976	**Applicant(s)** LUND, MARTIN	
	Examiner JOSEPH PAN	**Art Unit** 2492	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2011*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 August 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office Action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 10, 2011 has been entered.

2. Applicant's response filed on January 10, 2011 has been fully considered. Claims 1 and 12 have been amended. Claims 1-24 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthurs et al. (U.S. Patent No. 4,896,934), hereinafter "Arthurs", in view of Sawey (U.S. Patent No. 7,151,777 B2), and further in view of admitted prior art of Ross et al. (U.S. Patent No. 6,658,002 B1), hereinafter "Ross".

Referring to claim 1:

i. Arthurs teaches:

A method of providing physical port security in a digital communication system, comprising:

receiving a frame of digital data at a network device (see figure 3 'packet format', of Arthurs);

a destination port bit map based on the destination address information contained in said frame of digital data (see figure 3, element 'destination bit-map field'; and column 5, lines 50-54, of Arthurs);

generating a physical port availability bit map of allowed destination ports, wherein said physical port availability bit map is generated based on one or both of information in said received frame of digital data and/or port security information associated with said network device (see column 5, lines 58-65; column 6, lines 4-9; and column 7, lines 1-3, of Arthurs);

comparing, using at least one logical operation, said destination port bit map with said physical port availability bit map to generate a bit map of allowed destination ports (see column 5, lines 58-65; column 6, lines 4-9; and column 7, lines 1-3, of Arthurs); and

forwarding said frame of digital data to one or more of said allowed destination ports (see figure 1, elements 14-1..14-n 'output ports', of Arthurs).

Arthurs further discloses using the destination port bit map. However, Arthurs does not specifically mention generating the destination port bit map.

Arthurs discloses generating the physical port availability bit map. However, Arthurs does not specifically mention the physical port security bit map.

ii. Sawey teaches a crosspoint switch having multicast functionality, wherein Sawey discloses generating the destination port bit map based on the destination address contained in the frame of the digital data (see figure 4, elements 100 'receive multicast packet', 102 'generate port map mapping multicast address to destination output ports'; and column 7, lines 41-45, of Sawey).

On the other hand, Ross teaches a method for performing logical operations for packet processing, wherein Ross discloses generating a physical port security bit map based on information in said received frame of digital data (see column 3, line 58 to column 4, line 1 'Thus, if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number [i.e., a physical port security bit map]. Note that, as the rules are typically more complex than simple filters on port numbers, the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address [i.e., information of the packet], source port number, destination port number, type of service (TOS), and Layer 3 and Layer 4 protocol identification.', of Ross, emphasis added).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sawey into the system of Arthurs to generate a destination port bit map, because Arthurs teaches "The present invention relates to an optical switch for use in a fiber optic telecommunications network, and more particularly, to an optical switch with multicast capability." (see column 1, lines 5-8, of Arthurs, emphasis added). Arthurs further discloses "The Destination Bit Map Field indicates to which output ports a packet is to be sent. There is a bit d.sub.1. . .d.sub.N corresponding to each **possible** output port [i.e., the packet sender might use non-current output port information when setting the Destination Bit Map Field] 14-1 … 14-N. Setting d.sub.i =1 indicates that a copy of this packet is to be transmitted to the i.sup.th output port 14-i." (see column 5, lines 50-54, of Arthurs). Sawey teaches "The present invention relates generally to packet switching and, more particularly, to a crosspoint switch having multicast functionality." (see column 1, lines 6-8, of Sawey, emphasis added). Sawey further teaches "For example, multiplexor 20 may generate a revised port map (PM') that indicates recipients currently available [i.e., the multiplexer can use the current output port information to generate a reliable port map] to receive a copy of the multicast packet." (see column 7, lines 14-17, of Sawey). Arthurs further discloses "Specifically, the fan out of a multicast packet is the number of output ports that are destined to receive a copy of the packet. Because the output port contention probability increases rapidly as fan out increases, a multicast packet with large fan out will probably be blocked." (see column 7, lines 34-39, of Arthurs, emphasis added). Sawey further discloses "For example, multiplexor 20 may generate a revised port map (PM') that indicates recipients currently available to receive a copy of the multicast packet. Thus, as indicated at 54, multiplexor 20 may schedule the multicast packet for communication to available recipients by associating the revised port map with the multicast packet." (see column 7, lines 14-20, of Sawey, emphasis added). Therefore, Sawey's teaching could further enhance Arthurs's system, because Sawey's destination port bit map "indicates recipients currently available [i.e., current and dynamic] to receive a copy of the multicast packet", while Arthurs's destination port bit map is pre-generated and static, which does not "indicates recipients currently available to receive a copy of the multicast packet"

The ordinary skilled person would have been motivated to have applied the teaching of Ross into the system of Arthurs to generate the physical port security bit map, because Arthurs teaches "Illustratively, the electronic control network is in the form of a track which sequentially links all of the input ports and output ports. At the beginning of the track is a token generator which generates control tokens. The control tokens are passed sequentially around the track from port to port." (see column 2, lines 58-63, of Arthurs, emphasis added). Ross teaches "The present invention generally concerns data communications systems, in particular internetworking systems and specifically access control techniques for such systems." (see column 1, lines 13-15, of Ross, emphasis added). Therefore, Ross's teaching could enhance Arthurs's system, because "the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address [i.e., information of the packet], source port number, destination port number, type of service (TOS), and Layer 3 and Layer 4 protocol identification."

Referring to claims 2, 13:

Arthurs, Sawey, and Ross teach the claimed subject matter: a method of providing physical port security in a digital communication system (see claim 1 above). Arthurs further discloses the logical AND (see figure 13A; and column 5, line 64, of Ross).

Referring to claims 3-5, 14-16, 23:

Arthurs, Sawey, and Ross teach the claimed subject matter: a method of providing physical port security in a digital communication system (see claim 1 above). They further disclose the source address and the destination address (see column 3, line 58 to column 4, line 1, of Ross).

Referring to claims 6, 17, 22:

Arthurs, Sawey, and Ross teach the claimed subject matter: a method of providing physical port security in a digital communication system (see claim 1 above). Arthurs further discloses the IP address (see column 2, line 57, of Ross).

Referring to claims 7, 18:

Arthurs, Sawey, and Ross teach the claimed subject matter: a method of providing physical port security in a digital communication system (see claim 1 above). Arthurs further discloses the router (see column 2, lines 31-33, of Arthurs).

Referring to claims 8, 19:

Arthurs, Sawey, and Ross teach the claimed subject matter: an intermediate network device (see claim 12 above). They further disclose the network file server (see column 1, lines 51-52, of Ross).

Referring to claims 9, 20:

Arthurs, Sawey, and Ross teach the claimed subject matter: an intermediate network device (see claim 12 above). They further disclose the local area network (see column 1, line 35, of Ross).

Referring to claim 10:

Arthurs, Sawey, and Ross teach the claimed subject matter: a method of providing physical port security in a digital communication system (see claim 1 above). They further discloses the process (see column 1, line 51, of Sawey).

Referring to claim 11:

Arthurs, Sawey, and Ross teach the claimed subject matter: a method of providing physical port security in a digital communication system (see claim 1 above). Ross further discloses that the physical port security bit map is generated dynamically based on a variable parameter (see e.g. column 3, line 58 to column 4, line 1, of Ross).

Referring to claim 12:

i. Arthurs teaches:

A system for providing physical port security, comprising:

at least one processor within a network device, said network device having a communication port for receiving digital data from a digital communications system and two or more physical data ports for forwarding said digital data, said at least one of processor enables (see figure 1, element 10; and column 2, lines 31-33, of Arthurs):

a destination port bit map based on the destination address information contained in said frame of digital data (see figure 3, element 'destination bit-map field'; and column 5, lines 50-54, of Arthurs);

generating a physical port availability bit map of allowed destination ports, wherein said physical port availability bit map is generated based on one or both of information in said received frame of digital data and/or port security information associated with said network device (see column 5, lines 58-65; column 6, lines 4-9; and column 7, lines 1-3, of Arthurs);

comparing, using at least one logical operation, said destination port bit map with said physical port availability bit map to generate a bit map of allowed destination ports (see column 5, lines 58-65; column 6, lines 4-9; and column 7, lines 1-3, of Arthurs); and

forwarding of said digital data to one or more of said allowed destination ports (see figure 1, elements 14-1..14-n 'output ports', of Arthurs).

Arthurs discloses generating the physical port availability bit map. However, Arthurs does not specifically mention the physical port security bit map.

Arthurs further discloses using the destination port bit map. However, Arthurs does not specifically mention generating the destination port bit map.

ii. Sawey teaches a crosspoint switch having multicast functionality, wherein Sawey discloses generating the destination port bit map based on the destination address contained in the frame of the digital data (see figure 4, elements 100 ‘receive multicast packet’, 102 ‘generate port map mapping multicast address to destination output ports'; and column 7, lines 41-45, of Sawey).

On the other hand, Ross teaches a method for performing logical operations for packet processing, wherein Ross discloses generating a physical port security bit map based on information in said received frame of digital data (see column 3, line 58 to column 4, line 1 ‘Thus, if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number [i.e., a physical port security bit map]. Note that, as the rules are typically more complex than simple filters on port numbers, the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address [i.e., information of the packet], source port number, destination port number, type of service (TOS), and Layer 3 and Layer 4 protocol identification.’, of Ross, emphasis added).

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sawey into the system of Arthurs to generate a destination port bit map, because Arthurs teaches “The present invention relates to an optical switch for use in a fiber optic telecommunications network, and more particularly, to an optical switch with multicast capability.” (see column 1, lines 5-8, of Arthurs, emphasis added). Arthurs further discloses “The Destination Bit Map Field indicates to which output ports a packet is to be sent. There is a bit d.sub.1. . .d.sub.N corresponding to each **possible** output port [i.e., the packet sender might use non-current output port information when setting the Destination Bit Map Field] 14-1 … 14-N. Setting d.sub.i =1 indicates that a copy of this packet is to be transmitted to the i.sup.th output port 14-i.” (see column 5, lines 50-54, of Arthurs). Sawey teaches “The present invention relates generally to packet switching and, more particularly, to a crosspoint switch having multicast functionality.” (see column 1, lines 6-8, of Sawey, emphasis added). Sawey further teaches "For example, multiplexor 20 may generate a revised port map (PM') that indicates recipients currently available [i.e., the multiplexer can use the current output port information to generate a reliable port map] to receive a copy of the multicast packet." (see column 7, lines 14-17, of Sawey). Arthurs further discloses “Specifically, the fan out of a multicast packet is the number of output ports that are destined to receive a copy of the packet. Because the output port contention probability increases rapidly as fan out increases, a multicast packet with large fan out will probably be blocked.” (see column 7, lines 34-39, of Arthurs, emphasis added). Sawey further discloses “For example, multiplexor 20 may generate a revised port map (PM') that indicates recipients currently available to receive a copy of the multicast packet. Thus, as indicated at 54, multiplexor 20 may schedule the multicast packet for communication to available recipients by associating the revised port map with the multicast packet.” (see column 7, lines 14-20, of Sawey, emphasis added). Therefore, Sawey’s teaching could further enhance Arthurs’s system, because Sawey’s destination port bit map "indicates recipients currently available [i.e., current and dynamic] to receive a copy of the multicast packet", while Arthurs’s destination port bit map is pre-generated and static, which does not "indicates recipients currently available to receive a copy of the multicast packet"

The ordinary skilled person would have been motivated to have applied the teaching of Ross into the system of Arthurs to generate the physical port security bit map, because Arthurs teaches “Illustratively, the electronic control network is in the form of a track which sequentially links all of the input ports and output ports. At the beginning of the track is a token generator which generates control tokens. The control tokens are passed sequentially around the track from port to port.” (see column 2, lines 58-63, of Arthurs, emphasis added). Ross teaches “The present invention generally concerns data communications systems, in particular internetworking systems and specifically access control techniques for such systems.” (see column 1, lines 13-15, of Ross, emphasis added). Therefore, Ross’s teaching could enhance Arthurs’s system, because "the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address [i.e., information of the packet], source port number, destination port number, type of service (TOS), and Layer 3 and Layer 4 protocol identification."

Referring to claim 21:

Arthurs, Sawey, and Ross teach the claimed subject matter: an intermediate network device (see claim 12 above). They further disclose the IP data (see column 1, line 29 'data packet', of Ross).

Referring to claims 24:

Arthurs, Sawey, and Ross teach the claimed subject matter: an intermediate network device (see claim 12 above). Ross further discloses that the physical port security bit map is dynamically altered based on a variable parameter (see e.g. column 3, line 58 to column 4, line 1, of Ross).

Response to Arguments

5. Applicant's following arguments, filed on January 10, 2011, have been fully considered but they are not persuasive.

Re: claims 1 and 12:

(a) Applicant argues:

"However, the destination bitmap field of Arthurs is not generated "based on the destination address information contained in said frame of digital data," as required by the claims." (see page 10, 3rd paragraph).

Examiner maintains:

Arthurs discloses "The format of a packet arriving at one of the input ports 12 is shown in FIG. 3. Illustratively, the packet has four fields, a Data Field, a Source Address Field, a Destination Bit Map Field, and a Priority Bits Field." (see column 5, lines 43-45, of Arthurs). Therefore, Arthurs discloses the destination bit map. However, Arthurs does not explicitly discloses generating the destination bit map.

On the other hand, Sawey discloses "FIG. 4 is a flowchart illustrating the progression of a multicast packet within input module 12. Input module 12 receives the multicast packet at step 100. Input module 12 then generates a port map mapping the multicast address of the multicast packet to destination output ports at step 102 [i.e., generating a destination port bit map based on the destination address information contained in said frame of digital data]." (see column 7, lines 41-45, of Sawey).

Therefore, the combination of references discloses generating a destination port bit map based on the destination address information contained in said frame of digital data, such as claimed.

(b) Applicant argues:

"The mere fact that Sawey and Arthurs both have "multicast capabilities" does not provide a motivation to combine these references. The Examiner also makes the unsupported allegation that "Sawey's teaching could enhance Arthurs's (sic.) system." ." (see page 12, middle of the paragraph).

Examiner maintains:

The previous Office Action states "The ordinary skilled person would have been motivated to have applied the teaching of Sawey into the system of Arthurs to generate a destination port bit map, because Arthurs teaches "The present invention relates to an optical switch for use in a fiber optic telecommunications network, and more particularly, to an optical switch with multicast capability." (see column 1, lines 5-8, of Arthurs, emphasis added). Sawey teaches "The present invention relates generally to packet switching and, more particularly, to a crosspoint switch having multicast functionality." (see column 1, lines 6-8, of Sawey, emphasis added). Therefore, Sawey's teaching could enhance Arthurs's system.". Therefore, Examiner explained the motivation for making the combination of Arthurs and Sawey.

Additionally, Arthurs discloses "Specifically, the fan out of a multicast packet is the number of output ports that are destined to receive a copy of the packet. Because the output port contention probability increases rapidly as fan out increases, a multicast packet with large fan out will probably be blocked.” (see column 7, lines 34-39, of Arthurs, emphasis added). Sawey discloses “For example, multiplexor 20 may generate a revised port map (PM') that indicates recipients currently available to receive a copy of the multicast packet. Thus, as indicated at 54, multiplexor 20 may schedule the multicast packet for communication to available recipients by associating the revised port map with the multicast packet.” (see column 7, lines 14-20, of Sawey, emphasis added). Therefore, Sawey’s teaching could further enhance Arthurs’s system, because Sawey’s destination port bit map "indicates recipients currently available to receive a copy of the multicast packet", while Arthurs’s destination port bit map is pre-generated and static, which does not "indicates recipients currently available to receive a copy of the multicast packet"

(c) Applicant argues:

“The answer is that a person of ordinary skill in the art simply would not make this combination. There would be no need to "generate" a destination bit map if it already existed." .” (see page 12, end of the paragraph).

Examiner maintains:

A person of ordinary skill in the art simply would make this combination, because Arthurs’s destination port bit map is pre-generated and static, which does not "indicates recipients currently available to receive a copy of the multicast packet" taught by Sawey (see also (b) above).

(d) Applicant argues:

“Neither Arthurs nor Sawey, alone or in combination, disclose or suggest a "physical port security bit map of allowed destination ports," as required by this claim element. As such, they also do not disclose or suggest "comparing said destination port bit map with said physical port security bit map."” (see page 13, last paragraph).

Examiner maintains:

Arthurs discloses “The format of a typical token generated by the token generator 32 of FIG. 1 is illustrated in FIG. 3. A token comprises two fields, a Source Address

Field and an Output Availability Field [i.e., the physical port availability bit map]. The Output Availability Field comprises a bita.sub.i for each output port 14-i. A logic "1" in a particular bit position of the Output Availability Field indicates that the corresponding output port has been reserved. The token generator emits tokens with a cleared output availability field [i.e., generate and initialize the physical port availability bit map]…" (see column 5, line 58 to column 6, line 3, of Arthurs, emphasis added). However, Arthurs does not explicitly discloses a physical port security bit map.

On the other hand, Ross discloses "Thus, if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number [i.e., generating a physical port security bit map]. Note that, as the rules are typically more complex than simple filters on port numbers, the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address, source port number, destination port number [i.e., based on information in said received frame of digital data], type of service (TOS), and Layer 3 and Layer 4 protocol identification." (see column 3, line 58 to column 4, line 1, of Ross).

Therefore, the combination of references discloses generating a physical port security bit map based on information in said received frame of digital data, such as claimed.

(e) Applicant argues:

"The mere fact that Arthurs and Ross both relate to "access control techniques" does not provide a motivation to combine these references. The Examiner also makes the unsupported allegation that "Ross' teaching could enhance Arthurs's (sic.) system." (See Final OA, p. 5). The Examiner provides no explanation of exactly how Arthurs' system would allegedly be enhanced."" (see page 15, 1st paragraph).

Examiner maintains:

The previous Office Action states "The ordinary skilled person would have been motivated to have applied the teaching of Ross into the system of Arthurs to generate the physical port security bit map, because Arthurs teaches “Illustratively, the electronic control network is in the form of a track which sequentially links all of the input ports and output ports. At the beginning of the track is a token generator which generates control tokens. The control tokens are passed sequentially around the track from port to port.” (see column 2, lines 58-63, of Arthurs, emphasis added). Ross teaches “The present invention generally concerns data communications systems, in particular internetworking systems and specifically access control techniques for such systems.” (see column 1, lines 13-15, of Ross, emphasis added). Therefore, Rossn’s teaching could enhance Arthurs’s system.". Therefore, Examiner explains the motivation for making this combination.

Additionally, Arthurs discloses “The format of a typical token generated by the token generator 32 of FIG. 1 is illustrated in FIG. 3. A token comprises two fields, a Source Address Field and an Output Availability Field [i.e., the physical port availability bit map]. The Output Availability Field comprises a bita.sub.i for each output port 14-i. A logic "1" in a particular bit position of the Output Availability Field indicates that the corresponding output port has been reserved. The token generator emits tokens with a cleared output availability field [i.e., generate and initialize the physical port availability bit map]…” (see column 5, line 58 to column 6, line 3, of Arthurs, emphasis added).

Ross discloses “Thus, if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number [i.e., generating a physical port security bit map]. Note that, as the rules are typically more complex than simple filters on port numbers, the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address, source port number, destination port number [i.e., based on information in said received frame of digital data], type of service (TOS), and Layer 3 and Layer 4 protocol identification.” (see column 3, line 58 to column 4, line 1, of Ross).

Therefore, Ross’s teaching could further enhance Arthurs’s system, because Arthurs's physical port availability bit map is generated and initialized to make all output ports available, while Ross's physical port security bit map is generated utilizing rules., such as "deny packets from port 80". Thus, Ross's physical port availability bit map could enhance the system of Arthurs and Saway by providing network security.

(f) Applicant argues:

“However, even though Ross discloses ACL rule implementation using CAM entries, there is still no disclosure of generating a physical port security bit map of allowed destination ports."” (see page 16, last paragraph).

Examiner maintains:

Ross discloses “Thus, if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number [i.e., generating a physical port security bit map]. Note that, as the rules are typically more complex than simple filters on port numbers, the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address, source port number, destination port number [i.e., based on information in said received frame of digital data], type of service (TOS), and Layer 3 and Layer 4 protocol identification.” (see column 3, line 58 to column 4, line 1, of Ross).

Therefore, the reference(s) disclose generating a physical port security bit map, and that a physical port security bit map is generated based on information in a received frame of digital data, such as claimed.

(g) Applicant argues:

“Furthermore, Ross also does not disclose that a physical port security bit map is generated based on information in a received frame of digital data and/or port security information associated with the network device, as recited in Applicant's claim 1.” (see page 17, 1st paragraph).

Examiner maintains:

Ross discloses “Thus, if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number [i.e., generating a physical port security bit map]. Note that, as the rules are typically more complex than simple filters on port numbers, the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address, source port number, destination port number [i.e., based on information in said received frame of digital data], type of service (TOS), and Layer 3 and Layer 4 protocol identification.” (see column 3, line 58 to column 4, line 1, of Ross).

Therefore, the reference(s) disclose generating a physical port security bit map, and that a physical port security bit map is generated based on information in a received frame of digital data, such as claimed.

(h) Applicant argues:

“the Applicant submits that the combination of Arthurs, Sawey and Ross does not disclose the limitation of "comparing, using at least one logical operation, said destination port bit map with said physical port security bit map to generate a bit map of allowed destination ports," as recited by Applicant's claim 1.” (see page 17, 2nd paragraph).

Examiner maintains:

Arthurs discloses “Note that the packet at the input port with SA=1 is a multicast packet. In particular, its Destination Bit Map Field indicates that d.sub.7 =1 and d.sub.3 =1 so that this packet is to be routed to output ports 7 and 3 (i.e. output ports 14-7 and 14-3 of FIG. 1). Since, the token leaves the token generator 31 with a clear Output Port Availability field and the input port with SA=1 is the first input port reached by the token, a.sub.3 and a.sub.7 are set to logic "1" in the "Output Availability" field of the token, and the address "1" for the first input port is written into the subfields A3 and A7 of the Source Address Field [i.e., generating a bit map of allowed destination ports] of the token. The token then passes to the input port with SA=2 (corresponding to input port

12-2 in FIG. 1)." (see column 6, lines 53-64, of Arthurs). Therefore, Arthurs discloses: comparing, using at least one logical operation, said destination port bit map with said physical port availability bit map to generate a bit map of allowed destination ports. However, Arthurs does not specifically mention physical port security bit map.

Ross discloses "Thus, if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number [i.e., generating a physical port security bit map]. Note that, as the rules are typically more complex than simple filters on port numbers, the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address, source port number, destination port number [i.e., based on information in said received frame of digital data], type of service (TOS), and Layer 3 and Layer 4 protocol identification." (see column 3, line 58 to column 4, line 1, of Ross).

In addition, Ross teaches a logical operation unit for packet processing wherein Ross discloses "The present invention performs logical operations on fields within the flow label characterizing a received packet or frame of data and uses the results, along with other packet/frame-identifying data, to generate a more efficient content addressable memory (CAM) lookup key." (see column 5, line 64 to column 6, line 1, of Ross).

Therefore, the combination of references disclose "comparing, using at least one logical operation, said destination port bit map with said physical port security bit map to generate a bit map of allowed destination ports," as recited by Applicant's claim 1.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Joseph Thomas can be reached at 571-272-6776. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Zachary A Davis/
Primary Examiner, Art Unit 2492

/Joseph Pan/
Examiner, Art Unit 2492
March 13, 2011